Privacy and Security: Protecting Confidential Information at the Department
Frequently Asked Questions

1. What type of personal health information does the department collect, and why?

Reportable Diseases. The department collects information about people who have certain diseases or conditions in order to protect the public health. Typically the department wants to know about diseases that 1) spread from person to person or may have serious consequences to anyone who gets the disease; or 2) indicate unsafe conditions that cause other individuals to be sick or harmed; or 3) include cancers and birth defects that are of particular concern to the public and can highlight environmental or lifestyle problems in Colorado or 4) diseases such as autism or muscular dystrophy where information is being gathered to understand these diseases in Colorado.

Some of the information is sent to the department by hospital staff and individual doctors or other health care providers. See http://www.cdphe.state.co.us/dc/Medlist.pdf.

Laboratories also send in positive results for specific tests that may indicate one of these conditions. See http://www.cdphe.state.co.us/dc/Lablist.pdf.

Grant programs. The department also collects information on patients who receive health care services sponsored by public health programs. Most of these programs are funded by state or federal grant funds. These programs are in response to Colorado statutes or to Colorado community planning priorities to reduce disease and improve overall health. The information is used to evaluate effectiveness, and to provide summary reports back to the legislature or the federal government. Typical programs include Women, Infants and Children (WIC) and daycare nutrition programs, cancer or newborn screening programs, and services to children with special health care needs.

Licensure and Health System Oversight. The department collects information on residents of nursing homes, assisted living centers and other health care facilities as part of its licensure efforts and to assist Medicaid and Medicare rate setting. The department also supports Medicare and Medicaid certification efforts for Colorado facilities. Information is also collected when responding to complaints about facilities.

Vital Records. The department maintains birth, death, adoption, marriage and divorce records for Colorado. The department has the official records for all persons born in the state of Colorado and issues birth and death records. The department also oversees the Medical Marijuana program, approved by voters in November 2000, which authorizes the use of marijuana to alleviate certain debilitating medical conditions.

State Laboratory. The department has a laboratory that conducts tests for a number of diseases. It collects patient data and has test results for specimens that are processed.

Emergency Medical Services Testing. The department collects information on individuals who apply for certification as an emergency care worker, such as an ambulance driver.

Environmental Permits and Licenses. The department collects information on individuals and businesses, including owners who apply for hazardous waste or other air and water permits. It also collects information on persons submitting environmental tests.

Medical Visa. The department collects information from individuals who apply for medical or dental visas to work in Colorado areas, which have a shortage of medical workers. The information is used to approve applications and monitor compliance.

Employee and Vendor Records. The department collects tax and Social Security information, and health benefit information from its employees, contractors and vendors as required for payroll, benefit and contract processing.

2. **How does the department make sure the health information is kept confidential?**
The department has an extensive Privacy and Security Program that includes:
    - Department–wide policies and related procedures on maintaining confidentiality and protecting information
    - Required health divisions medical privacy course
    - Required department-wide security course
    - Staff security reminders and updates
    - New employee brochure and training on privacy and security
    - Security engineer and technical staff to maintain information system protections
    - Continuity of operations plan for maintaining key services in an emergency
    - Privacy and Security Board that reviews the security program and advises the Chief Security Officer
    - Privacy Officer who advises programs on privacy issues and develops policies and procedures for staff, and training.
    - Security incident procedures
    - Contract provisions for vendors and subcontractors working for the department
    - Confidentiality agreements and procedures for approving access to department information systems.

    The department seeks to maintain compliance with international and national security standards.

3. **What about the Colorado Open Records Act…are all personal and health records protected?**
The Colorado Open Records Act protects personal and health information from being disclosed. In addition, Colorado state statutes offer additional protection for specific kinds of personal and health information (Vital records, HIV, mental health records, etc.) There are instances though when personal information may become subjected to a court subpoena or legal requirement. The department consults its own legal advisors and those of the Office of the Attorney General in these instances.

4. **What happens if there is a security breach? Will I be notified?**
The department has incident response procedures that include notifying persons whose information has been compromised.

5. **Has the department had a security audit? What were the results?**
The Legislative Council's State Auditor Office has audited several department programs. The more recent audits have included a review of privacy and security procedures. The results of those audits have been made public.
http://www.leg.state.co.us/OSA/coauditor1.nsf/ReportPublicDept?OpenForm

    Select the entry for the Colorado Department of Public Health and Environment to see reports from the State Auditor's Office and the department response to findings.

    In addition, the department hired a leading security firm to evaluate its security. The results of the audits have guided the department's Privacy and Security program. Details of the audit are kept confidential in order to limit outside knowledge of the security plans for the department. This is in accordance with the Colorado Open Records Act that limits access to network and security plans.

6. **Does personal health information get disclosed to anyone outside of the department?**
The department collects health information for a number of public health programs, from birth certificates, to nursing home licensure to the investigation of reportable communicable diseases. Health information may be made available to county level public health officials. Examples would include sharing information with local authorities who can issue birth certificates, or who are

responding to a food poisoning incident in the county, or who are running local clinics that provide services under grants from the department. In some instances information may be shared with health care providers treating a communicable disease, or with federal authorities leading an investigation into a disease outbreak. Information may be shared for scientific research purposes with the approval of an Institutional Review Board, set up to review human subjects research. Furthermore, there are department programs that are coordinated with services managed by other agencies, and in some cases, information needed for eligibility determinations may be shared with other programs. Finally, auditors and government officials who review department operations may be given access to information to the extent it relates to a program audit.

Medical information is de-identified when generating statistics used for public reporting. The department does not disclose health information to the public so that an individual can be identified and confidentiality compromised. The department does not provide health data to any state or local agencies involved with enforcement.

7. How is personal medical information used?

Personal medical information is used to assess the public health, and used to intervene so that others of the public will not be subject to similar diseases or conditions. Examples include investigating food poisoning, investigating cases of whooping cough or other vaccine preventable diseases, measuring how common autism is in Colorado and investigating quality issues in health care facilities.

8. Is the personal medical information used for research?

The vast majority of information that is collected is not used for research. If a research program requests medical information for research, the research must get approval from a federally sanctioned Institutional Review Board (IRB). The IRB will review the proposal and determine if the research proposal is appropriate and whether individual authorizations are needed from participants.

9. Why does the department collect personally identifiable medical information?

Colorado state statutes and regulations require the department to collect personally identifiable medical information for tracking diseases which impact public health, such as individuals with communicable diseases like hepatitis or tuberculosis. The laboratory also collects patient data and test results on specimens that are processed.

10. What legal protections are in place for the personal health information that the department collects?

Typically the statutes that authorize the department to operate public health programs also require that health information be kept confidential, and limit uses of the medical records. The Colorado Open Records Act also protects health information. Various federal statutes and rules that fund department programs also have additional requirements regarding maintaining confidentiality. The department is a public health authority and therefore has an exemption under the Health Insurance Portability and Accountability Act (HIPAA) to use personal health information. However, the department does protect data in accordance with HIPAA standards. Finally, department employees who violate department privacy and security policies and procedures are subject to discipline under the State of Colorado Personnel Rules. Sanctions may range from counseling by a supervisor and the assignment of additional training up to disciplinary actions including dismissal. Any individual who violates a federal, state or local law may expect that the department will refer that violation to the appropriate law enforcement agency for potential prosecution.

11. What process does the department have to go through before it can collect medical information?

The process varies with the reason for the collection of information. For mandatory disease reporting by physicians, hospitals or laboratories, the request for changes in what is reported must be reviewed and approved by the State Board of Health and is subject to public review and comment. In addition, new programs that collect medical information will be required to fill out a Privacy Impact Assessment. The Privacy Impact Assessment documents what information is collected, why, safeguards and how the information will be used and disclosed. The use of Privacy Impact

Assessments is new and training on the form and procedures is being planned. PIAs will be accessible via the Internet at the department's web site beginning fall 2006.

12. **What is a Privacy Impact Assessment, and why are they important?**
    Privacy Impact Assessments allow the department to notify citizens as to how information is collected, protected, and used. It is another way of making sure that citizens know what is being collected and why. It is also part of an internal review so that new programs think through and justify the information that is collected, and limit collection to the minimum necessary needed to protect the public health.

13. **Why would the department contact me?**
    If the department discovers through state required laboratory testing that a child has a newborn genetic or hearing disorder, parents will be contacted for medical follow-up. Individuals may be contacted if they are diagnosed with or potentially exposed to a reportable communicable disease. Individuals may also be contacted through random-digit dialing by the department's survey unit or through an IRB-approved research study (see question #9).

14. **If we have concerns about confidentiality, or general questions about privacy, whom can we contact at the department?**
    The Privacy Officer can be reached either by e-mail at cdphepofeedback@cdphe.state.co.us or by phone (303) 692-2311.